Listing of Claims

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently amended): A method for securing an accessible computer system, the method comprising:

monitoring for connection transactions between multiple access requestors and ~~multiple~~ access providers using a switching component connected to the ~~multiple~~ access providers, wherein the monitoring includes detecting connection transactions between multiple Internet protocol addresses and the access providers with the switching component; and

denying access by an attacking access requestor to the access providers when a number of connection transactions initiated by the attacking access requestor through the switching component exceeds a configurable threshold number during a first configurable period of time.

2. (Previously presented): The method as in claim 1, wherein the monitoring includes detecting connection transactions initiated by the access requestors through the switching component.

3. (Previously presented): The method as in claim 2, wherein the monitoring further includes counting the number of connection transactions initiated by the access requestors through the switching component during the first configurable period of time.

4. (Previously presented): The method as in claim 3, wherein the monitoring further includes comparing the number of connection transactions initiated by the access requestors through the switching component during the first configurable period of time to the configurable threshold number.

5. (Canceled)

6. (Currently amended): The method as in claim [[5]] 1 , wherein the monitoring further includes counting the number of connection transactions initiated through the switching component by the Internet protocol addresses during the first configurable period of time.

7. (Previously presented): The method as in claim 6, wherein the monitoring further includes comparing the number of connection transactions initiated by the Internet protocol addresses through the switching component during the first configurable period of time to the configurable threshold number.

8. (Original): The method as in claim 6, wherein the monitoring includes monitoring a computer system for connection transactions made using TCP.

9. (Currently amended): The method as in claim [[5]] 1, wherein the detecting includes identifying the Internet protocol addresses through the use of a header attached to a message representing the connection transaction being detected.

10. (Previously presented): The method as in claim 1, wherein the denying of access includes denying access to the access providers through the switching component by the attacking access requestor for a second configurable period of time.

11. (Previously presented): The method as in claim 10, wherein the denying of access further includes resetting the second configurable period of time after detecting a new connection transaction initiated by the attacking access requestor through the switching component during the second configurable period of time.

12. (Previously presented): The method as in claim 1, wherein the denying of access includes denying access to the access providers through the switching component by the attacking access requestor for a second configurable period of time after detecting a most recent

connection transaction initiated by the attacking access requestor through the switching component.

13. (Previously presented): The method as in claim 1, wherein the access requestors are clients and the access providers are hosts such that the monitoring includes detecting connection transactions through the switching component between multiple clients and multiple hosts.

14. (Currently amended): The method as in claim 3, wherein the counting further comprises counting a cumulative number of connection transactions for the ~~multiple~~ access providers connected to the switching component initiated by each of the access requestors during the first configurable period of time.

15. (Currently amended): A system for securing an accessible computer system, comprising:

a switching component connected to ~~multiple~~ access providers having means for:

monitoring for connection transactions between multiple access requestors and the ~~multiple~~ access providers, wherein the monitoring includes detecting connection transactions between multiple Internet protocol addresses and the access providers with the switching component; and

denying access by an attacking access requestor to the access providers when a number of connection transactions initiated by the attacking access requestor exceeds a configurable threshold number during a first configurable period of time.

16. (Previously presented): The system of claim 15, wherein the switching component includes:

means for detecting connection transactions initiated by the access requestors through the switching component;

means for counting the number of connection transactions initiated by the access requestors through the switching component during the first configurable period of time; and means for comparing the number of connection transactions initiated by the access requestors through the switching component during the first configurable period of time to the configurable threshold number.

17. (Currently amended): The system of claim 15, wherein the switching component includes:

means for detecting connection transactions between the multiple Internet protocol addresses and the access providers using the switching component;

means for counting the number of connection transactions initiated by the Internet protocol addresses through the switching component during the first configurable period of time; and

means for comparing the number of connection transactions initiated by the Internet protocol addresses through the switching component during the first configurable period of time to the configurable threshold number.

18. (Original): The system of claim 17, wherein the means for monitoring includes means for monitoring a computer system for connection transactions made using TCP.

19. (Previously presented): The system of claim 17, wherein the means for detecting includes:

means for identifying the Internet protocol addresses through the use of a header attached to a message representing the connection transaction being detected.

20. (Previously presented): The system of claim 15, wherein the switching component includes:

means for denying access to the access providers through the switching component by the attacking access requestor for a second configurable period of time.

21. (Previously presented): The system of claim 20, wherein the means for denying access further includes:

means for resetting the second configurable period of time after detecting a new connection transaction initiated by the attacking access requestor through the switching component during the second configurable period of time.

22. (Previously presented): The system of claim 15, wherein the means for the switching component includes:

means for denying access to the access providers through the switching component by the attacking access requestor for a second configurable period of time after detecting a most recent connection transaction initiated by the access requestor.

23. (Previously presented): The system of claim 15, wherein the access requestors are clients and the access providers are hosts such that the means for the switching component includes:

means for detecting connection transactions through the switching component between multiple clients and multiple hosts.

24. (Currently amended): The system of claim 16, wherein the means for counting further comprises means for counting a cumulative number of connection transactions for the ~~multiple~~ access providers connected to the switching component initiated by each of the access requestors during the first configurable period of time.

25. (Currently amended): A system for securing an accessible computer system, comprising:

a switching component connected to ~~multiple~~ access providers to:

monitor for connection transactions between multiple access requestors and ~~multiple~~ access providers, wherein to monitor for connection transactions include to detect connection transactions between multiple Internet protocol addresses and the access providers with the switching component; and deny access by the access requestor to the access providers when a number of connection transactions initiated by an attacking access requestor exceed a configurable threshold number during a first configurable period of time.

26. (Previously presented): The system of claim 25, wherein the switching component comprises:

a detection component that is structured and arranged to detect connection transactions initiated by the access requestors through the switching component;

a counting component that is structured and arranged to count the number of connection transactions initiated by the access requestors through the switching component during the first configurable period of time; and

a comparing component that is structured and arranged to compare the number of connection transactions initiated by the access requestors through the switching component during the first configurable period of time to the configurable threshold number.

27. (Currently amended): The system of claim 25, wherein the switching component comprises:

a detection component that is structured and arranged to detect connection transactions through the switching component between the multiple Internet protocol addresses and the access providers;

a counting component that is structured and arranged to count the number of connection transactions initiated through the switching component by the Internet protocol addresses during the first configurable period of time; and

a comparing component that is structured and arranged to compare the number of connection transactions initiated through the switching component by the Internet protocol addresses during the first configurable period of time to the configurable threshold number.

28. (Original): The system of claim 27, wherein the connection transactions include connections made using TCP.

29. (Previously presented): The system of claim 27, wherein the detection component comprises:

an identifying component that is structured and arranged to identify the Internet protocol addresses through the use of a header attached to a message representing the connection transaction being detected.

30. (Previously presented): The system of claim 25, wherein the switching component comprises:

an access preventer that is structured and arranged to deny access to the access providers through the switching component by the attacking access requestor for a second configurable period of time.

31. (Previously presented): The system of claim 30, wherein the switching component further comprises:

a timing component that is structured and arranged to measure the second configurable period of time during which the access preventer denies access to the access providers by the attacking access requestor.

32. (Previously presented): The system of claim 31, wherein the switching component further comprises:

a reset component that is structured and arranged to reset the timing component after detecting a new connection transaction initiated by the attacking access requestor through the switching component during the second configurable period of time.

33. (Previously presented): The system of claim 25, wherein the switching component comprises:

an access preventer that is structured and arranged to deny access to the access providers through the switching component by the attacking access requestor for a second configurable period of time after detecting a most recent connection transaction initiated by the access requestor.

34. (Previously presented): The system of claim 25, wherein the access requestors are clients and the access providers are hosts such that the switching component comprises:

a detection component that is structured and arranged to detect connection transactions through the switching component between multiple clients and multiple hosts.

35. (Currently amended): The system of claim 26, wherein the counting component further comprises counting a cumulative number of connection transactions for the ~~multiple~~ access providers connected to the switching component initiated by each of the access requestors during the first configurable period of time.

36. (Previously presented): The system of claim 25, wherein a host computer system receives communications from the switching component.

37. (Previously presented): The system of claim 25, wherein the switching component is included in a host computer system.